

SWITCH AND LAN

Publication number: JP2003348113

Publication date: 2003-12-05

Inventor: HOSOHARA TAKESHI

Applicant: HOSOHARA TAKESHI

Classification:

- international: G06F21/22; G06F11/00; H04L12/46; H04L12/66;
G06F21/22; G06F11/00; H04L12/46; H04L12/66; (IPC1-7): H04L12/46; G06F11/00; H04L12/66

- European:

Application number: JP20020147651 20020522

Priority number(s): JP20020147651 20020522

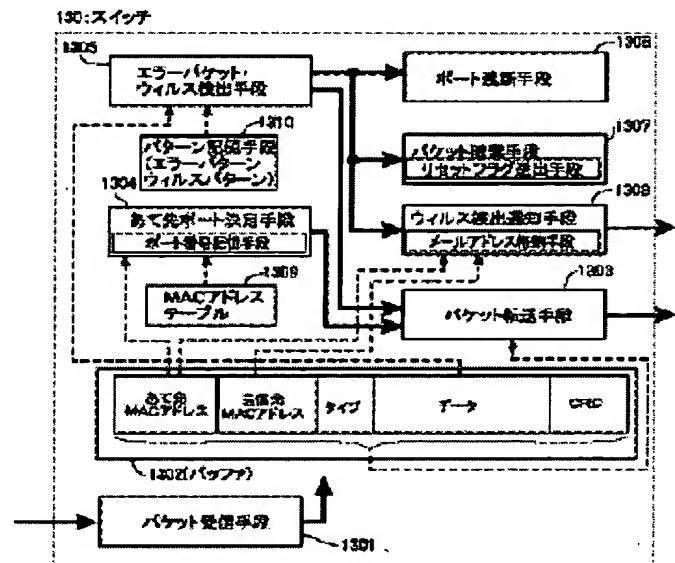
Report a data error here

Abstract of JP2003348113

PROBLEM TO BE SOLVED: To prevent illegal packets (computer virus or the like) from being spread and expanded by detecting transmission of the illegal packets from an inside of a LAN to a WAN or delivery of them between computers in the LAN.

SOLUTION: A switch of this invention includes: (1) an illegal pattern detection means (error packet/virus detection means 1305) for detecting illegal packets from packets transmitted from computers in the LAN 100 to a WAN access apparatus and/or packets delivered among in-LAN computers; and (2) at least one of ((1)) a port shut-off means (1306) for shutting off a port, ((2)) an illegal packet abort means (1307) for aborting illegal packets, and ((3)) an illegal packet detection notice means (1308) for informing at least either of a management computer sender computer and a destination computer about detection of the illegal packets, when the illegal pattern detection means detects the illegal packets.

COPYRIGHT: (C)2004,JPO



Data supplied from the esp@cenet database - Worldwide

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号
特開2003-348113
(P2003-348113A)

(43)公開日 平成15年12月5日(2003.12.5)

(51)Int.Cl.⁷
H 0 4 L 12/46
G 0 6 F 11/00
H 0 4 L 12/66
識別記号
2 0 0F I
H 0 4 L 12/46
12/66
G 0 6 F 9/06
テ-マコト*(参考)
E 5 B 0 7 6
2 0 0 S 5 K 0 3 0
B 5 K 0 3 3
6 6 0 N

審査請求 未請求 請求項の数5 OL (全 6 頁)

(21)出願番号 特願2002-147651(P2002-147651)

(22)出願日 平成14年5月22日(2002.5.22)

(71)出願人 502183382

細原 豪

東京都世田谷区松原6-36-17 マツモク
レスト201

(72)発明者 細原 豪

東京都世田谷区松原6-36-17 マツモク
レスト201

(74)代理人 100094488

弁理士 平石 利子

Fターム(参考) 5B076 FD08

5K030 GA15 HA08 HD06 LC18

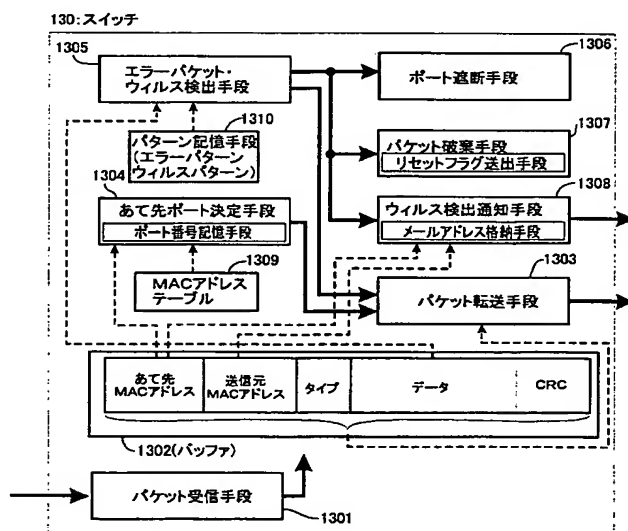
5K033 AA08 DA06 DB18 EC04

(54)【発明の名称】 スイッチおよびLAN

(57)【要約】

【課題】 不正パケット（コンピュータウイルス等）の、LAN内からWANへの送出や、LAN内のコンピュータ間での受け渡しを検出することで、当該不正パケットの拡散拡大等を防止する。

【解決手段】 (1) LAN100内コンピュータからWAN接続装置に送出されるパケットおよび／またはLAN内コンピュータ間で受け渡しされるパケットから不正パケットを検出する不正パターン検出手段（エラーパケット・ウイルス検出手段1305）、(2) 不正パターン検出手段が不正パケットを検出したときに、①ポートの遮断を行うポート遮断手段（1306）、②不正パケットを破棄する不正パケット破棄手段（1307）、③不正パケットの検出を管理コンピュータ送信元コンピュータ、あて先コンピュータの少なくとも1つに通知する不正パケット検出通知手段（1308）、の少なくとも一つの手段、を備える。



【特許請求の範囲】

【請求項 1】 局所ネットワーク内の少なくとも 1 つのコンピュータを広域ネットワーク接続装置に接続し、または当該局所ネットワーク内の所定のコンピュータ間を接続するスイッチであって、前記コンピュータから広域ネットワーク接続装置に送出されるパケット、および／または前記コンピュータ間で受け渡しされるパケットから不正パケットを検出する不正パターン検出手段、および、前記不正パターン検出手段が前記不正パケットを検出したときに、

ポートの遮断を行うポート遮断手段、

前記不正パケットを破棄する不正パケット破棄手段、前記不正パケットの検出を管理コンピュータ、送信元コンピュータ、あて先コンピュータの少なくとも 1 つに通知する不正パケット検出通知手段、の少なくとも一つの手段、を備えてなることを特徴とするスイッチ。

【請求項 2】 前記不正パターン検出手段は、複数の不正パターンを記憶する不正パターン記憶手段と、

前記不正パターン記憶手段に記憶された各不正パターンとパケットデータとを比較する比較手段と、を備えたことを特徴とする請求項 1 に記載のスイッチ。

【請求項 3】 広域ネットワークを介して接続された不正パケットデータベースホスト装置から複数の不正パターンを取得して蓄積する不正パターンデータベースと、前記不正パターンデータベースに蓄積された不正パターンが複数セットされる請求項 1 または 2 に記載のスイッチと、を備えたことを特徴とする局所ネットワーク。

【請求項 4】 前記不正パターンデータベースに蓄積された不正パターンが複数セットされる不正パケット検出サーバを介して、前記広域ネットワークに接続されてなることを特徴とする請求項 3 に記載の局所ネットワーク。

【請求項 5】 前記スイッチにセットされた複数の不正パターンと、前記不正パケットチェックサーバにセットされた複数の不正パターンとが、少なくとも一部が異なるように選ばれてなることを特徴とする請求項 3 または 4 に記載の局所ネットワーク。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、不正パケット（コンピュータウイルス等）の、局所ネットワーク（LAN）内から広域ネットワーク（WAN）への送出や、LAN 内のコンピュータ間での受け渡しを検出することで、当該不正パケットの拡散拡大等を防止することができるスイッチおよび局所ネットワークに関する。

【0002】

【従来の技術】 いわゆるワクチン・ソフトをインターネットに接続された LAN 内の端末コンピュータやブロッ

クサーバ（以下、「端末コンピュータ等」と言う）に導入することで、LAN 内の端末コンピュータ等をウィルスの感染から防ぐことができ、また、ウイルスに感染したファイルを修復することができる。

【0003】 ところが、上記のようなウイルス対策を、端末コンピュータ等において個別に行う場合には、各端末コンピュータ等のすべてに、ワクチン・ソフトを導入しなければならない。しかも、新種ウイルスに対しては、ワクチン・ソフトをそれぞれ頻繁にバージョンアップせねばならない。

【0004】 特に、端末コンピュータ側でウイルスの監視を行う場合には、新種ウイルスのパターンの更新やウイルスチェックの時期設定は、端末コンピュータのユーザに任せられるため、LAN における完全なウイルス対策を実現することは容易ではない。

【0005】 このために、LAN 側のインターネットとの接続経路中にウイルスチェックサーバを配置し、ウイルスの侵入を未然に防ぐこともと行われている。この種のウイルスチェックサーバは、通過するパケットのデータをバッファに取り込み、予めレジスタ等にセットされているウイルスパターンと比較し、ウイルスチェックを行う。これにより、原理上は各端末コンピュータをウイルスの感染から防ぐことができる。

【0006】

【発明が解決しようとする課題】 しかし、実際には、ウイルスチェックサーバにトラフィックが集中した場合には、ウイルスチェックの取りこぼしが生じることがある。また、ウイルスチェックサーバでは、LAN 内でのコンピュータ間同士でのウイルスの感染を防止することができない。

【0007】 本発明の目的は、コンピュータウイルス等の不正パケットの LAN から WAN への送出、または LAN 内のコンピュータ間での不正パケットの受け渡しを検出することで、当該不正パケットの拡散を防止することができるスイッチおよび LAN を提供することにある。

【0008】

【課題を解決するための手段】 本発明のスイッチは、LAN 内の少なくとも 1 つのコンピュータを WAN 接続装置に接続し、または当該 LAN 内の所定のコンピュータ間を接続するものであって、前記コンピュータから WAN 接続装置に送出されるパケット、および／または前記コンピュータ間で受け渡しされるパケットからコンピュータウイルスにかかる不正パケットを検出する不正パターン検出手段、および、前記不正パターン検出手段が前記不正パケットを検出したときに、ポートの遮断を行うポート遮断手段（ポートからのコンピュータの遮断、ポート自体を使用不可とする処理を含む）、前記不正パケットを破棄する不正パケット破棄手段、前記不正パケットの検出を管理コンピュータ、送信元コンピュータ、あ

て先コンピュータの少なくとも1つに通知する不正パケット検出通知手段の少なくとも一つの手段を備えてなることを特徴とする。

【0009】本発明では、スイッチを経由して転送されるパケットに含まれる不正パターンをスイッチが検出するので、たとえばウイルスチェックサーバや端末コンピュータに導入されているウイルスチェックソフトによるウイルス検出に取りこぼしが発生するような場合であっても、極力ウイルスの検出の確度を高めることができる。なお、不正パケット検出通知手段は、管理コンピュータ、送信元コンピュータ、あるいは、あて先コンピュータに送信するときは、たとえばパケットに含まれるIPアドレスに基づき各コンピュータに通知を行うことができる。この場合には、通知先のコンピュータ側に対応する通信アプリケーションが備えられる。

【0010】また、本発明のスイッチでは、前記不正パターン検出手段は、複数の不正パターンを記憶する不正パターン記憶手段と、前記不正パターン記憶手段に記憶された各不正パターンとパケットデータとを比較する比較手段とを備えることができる。

【0011】また、本発明のLANは、WANを介して接続された不正パケットデータベースホスト装置からコンピュータウイルス等の不正パターンを複数取得して蓄積する不正パターンデータベースと、前記不正パターンデータベースに蓄積された不正パターンが複数セットされる上記のスイッチとを備えたことを特徴とする。

【0012】本発明のLANは、不正パターンデータベースに蓄積された不正パターンが複数セットされる不正パケット検出サーバを介して、前記WANに接続することができる。この場合、不正パケット検出サーバと、本発明のスイッチとは、同一の不正データパターンをチェックすることもできるし、非同一の（異なる）不正データパターンをチェックすることもできる。不正パケット検出サーバと、本発明のスイッチとが、非同一または一部非同一（一部同一）の不正パターンをチェックすることでLANシステム全体の不正パターンチェック動作の最適化を図ることができる。

【0013】

【発明の実施の形態】図1は本発明のLANが、WAN（インターネット）に接続されたシステムの説明図である。

【0014】図1においてインターネット200には、ゲートウェイGW1を介してLAN100が接続され、ゲートウェイGW2を介してウイルスパターンデータベースサーバ300が接続されている。LAN100は、ウイルスチェックサーバ11と、コアスイッチ12と、複数のスイッチ（図1では符号131、132で示される2つを示す）とを備えている。

【0015】図1ではウイルスチェックサーバ11は、ウイルスパターンデータベースサーバ300からウイル

スパターンを一定時間間隔でダウンロードしており、通過するパケットから所定のウイルスを検出することができる。

【0016】図1のLAN100において、コアスイッチ12にはスイッチ131、132が分岐接続され、それぞれのスイッチ131、132には端末コンピュータやハブが接続可能に構成されている。図1では、説明の便宜上、スイッチ131に接続された端末コンピュータ1411、1412およびハブ1413が、スイッチ132に接続された端末コンピュータ1421、1422およびハブ1423がそれぞれ示されている。

【0017】また、スイッチ131、132には、ウイルスデータベース151、152がそれぞれ接続されている。図1では、スイッチ131、132は、ウイルスデータベース151、152に、ウイルスパターンデータベースサーバ300から、ウイルスパターンを一定時間間隔でダウンロードしている。

【0018】図2は、スイッチ131、132（図2では符号130で示す）の機能ブロック図であり、パケット受信手段1301と、パケットバッファ1302と、パケット転送手段1303と、あて先ポート決定手段1304と、エラーパケット・ウイルス検出手段（本発明の不正パターン検出手段としても機能する）1305と、ポート遮断手段1306と、パケット破棄手段（本発明の不正パケット破棄手段としても機能する）1307と、ウイルス検出通知手段（本発明の不正パケット検出通知手段）1308と、MACアドレステーブル1309と、パターン記憶手段1310とを備えている。

【0019】あて先ポート決定手段1304は、ポート番号記憶手段を備えており、ウイルス検出通知手段1308は、管理コンピュータのメールアドレスを格納する手段を備えることができ、パケット破棄手段1307は、パケットを廃棄したときにリセットフラグ（パケットを破棄した旨を示す信号）を送出するリセットフラグ送出手段を備えることができる。また、MACアドレステーブル1309には、図3（C）、（D）に示すように、ポート番号と、各ポートに接続された端末コンピュータ等のMACアドレスが記録される（なお、コアスイッチ12も、図3（B）に示すようなMACアドレステーブルを有している）。

【0020】あて先ポート決定手段1304は、MACアドレステーブル1309を参照して、あて先ポートを決定することができる。あて先ポート決定手段1304は、MACアドレステーブル1309にあて先のMACアドレスが書き込まれていないときは、ポートに接続されている端末コンピュータ等の全てにパケットを送信する（すなわち、フラッディングを行う）。あて先ポート決定手段1304は、あて先記憶手段を備えており、決定したあて先は当該記憶手段に一時記憶される。

【0021】以下に、図2のスイッチ130の作用を、

図3および一部図4を参照して説明する。なお、スイッチ130の処理の全部をソフトウェアで行うこともできるし、処理の全部または一部をハードウェア(ASIC)で行うこともできる。

【0022】図3(A)は、パケットフォーマットを示している。パケット受信手段1301がパケットを受信すると、当該パケットはパケットバッファ1302に格納される。

【0023】パケットバッファ1302にパケットが取り込まれたときは(図4のS101)、エラーパケット・ウイルス検出手段1305は、パターン記憶手段1320に記憶されたエラーパターンを参照して、受信したパケットのエラーパターンをチェックする(S102)。受信したパケットがエラーパケットである場合(S103の「YES」)には、当該パケットを破棄し(S104)、エラーパケットでない場合(S103の「NO」)には、エラーパケット・ウイルス検出手段1305は、パターン記憶手段1320に記憶されたウイルスパターンを参照して、受信したパケットのウイルスパターンのチェックを行う(S105)。ウイルスパターンが検出されないときは(S106の「NO」)、パケット転送手段1303は、宛先ポート決定手段1304の決定に従って宛先MACアドレスに対応するポート(あて先記憶手段に記憶されているポート番号に応じたポート)にパケットを送信する(S107)。

【0024】ステップS105においてウイルスパターンが検出されたときは(S106の「NO」)、①送信元コンピュータが接続されているポートの遮断スクリプト、②パケット破棄スクリプト、③LAN100内の管理コンピュータへのウイルス検出の通知(警告)スクリプトの少なくとも一つのスクリプトによる処理を選択し

(S108)、当該選択した処理を実行する(S109)。なお、①のスクリプトは図2のポート遮断手段1306に、②のスクリプトは図2のパケット破棄手段1307に、③のスクリプトは図2のウイルス検出通知手段108に対応する。これらのスクリプトのどれを選択するかは、たとえばスイッチの管理者(あるいはシステムの管理者)等が、予め設定できる。また、上記管理者等が、適宜そのスクリプトの定義等(ポート遮断を即時に行うかの設定、警告の内容定義等)の変更ができるようにすることが好ましい。

【0025】パケット破棄手段1307は、パケットを破棄するときは、リセットフラグ送出手段によりパケット送信元の端末コンピュータにリセットフラグを送出することができる。

【0026】LAN100内の管理コンピュータは、③におけるウイルス検出の通知を受けることで、LAN100内の、どの端末コンピュータがウイルスによる感染したかを、通知に含まれるMACアドレスを参照して知ることができ、通知されたMACアドレスからLAN1

00内でのウイルス感染の経路や感染状況を把握することができる。通常は、エラーパケット・ウイルス検出手段1305によるウイルス検出よりも前に、パケットが送信されることはない。しかし、スイッチ130にトラフィックが集中すること等により、エラーパケット・ウイルス検出手段1305によるウイルス検出がパケットのポートからの送信に間に合わず、パケット送信後にウイルスが検出されることもある。この場合には、ポート遮断を直ちに行い、またはウイルス検出通知手段108による通知の後にポート遮断を速やかに行うことができる。

【0027】上記の例では、ウイルス検出通知手段108は、ウイルス検出を管理コンピュータに通知しているが、パケットに含まれるIPアドレスに基づき、送信元コンピュータ、あるいは、あて先コンピュータにウイルス検出を通知することもできる。この場合には、通常、送信元コンピュータ、あるいは、あて先コンピュータにコンピュータに対応する通信アプリケーションを導入しておく必要がある。

【0028】図1に示したシステムでは、ゲートウェイGW1にトラフィックが集中した場合には、ウイルスチェックサーバ11におけるウイルス検出に取りこぼしが生じることがある。エラーパケット・ウイルス検出手段1305がウイルスチェックに際して参照するウイルスパターンと、ウイルスチェックサーバ11がウイルスチェックに際して参照するウイルスパターンとを同一とすることで、上記の取りこぼしによるウイルス感染を回避することができる。もちろん、エラーパケット・ウイルス検出手段1305がウイルスチェックに際して参照するウイルスパターンと、ウイルスチェックサーバ11がウイルスチェックに際して参照するウイルスパターンとを非同一または一部非同一とすることで、システム全体のウイルス検出の最適化を図ること(これにより転送速度が低下することを防止すること)ができる。なお、上記実施形態では、コアスイッチ12はウイルス検出機能は備えていないが、コアスイッチ13にウイルス検出機能を持たせることもできる。

【0029】

【発明の効果】本発明のスイッチでは、コンピュータウイルス等の不正パケットのLANからWANへの送出、またはLAN内のコンピュータ間での不正パケットの受け渡しを検出し、不正パケットが検出されたときはポートの遮断、管理コンピュータへの通知をただちに行うので、当該不正パケットの拡散を効率よく防止することができる。

【0030】本発明のLANシステムでは、ウイルスチェックサーバによりウイルスのチェックを行うとともに本発明のスイッチによりウイルスのチェックを行うことができるので、ウイルスチェックをより完全に行うことができる。しかも、LAN内の端末コンピュータ間でや

り取りされるパケットについてウイルスチェックを行うので、LAN内での感染拡大を防止することができる。

【図面の簡単な説明】

【図1】本発明の一実施形態を示すネットワークシステムを示す図である。

【図2】本発明のスイッチの一実施形態を示す機能ブロック図である。

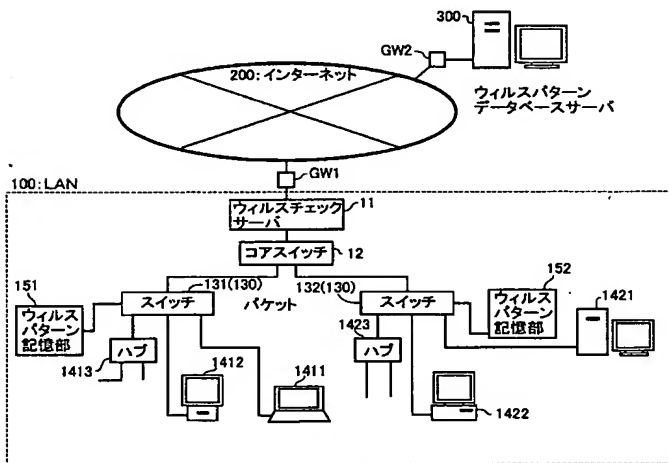
【図3】(A)はパケットのフォーマット図、(B)～(D)はスイッチのMACアドレステーブルを示す図である。

【図4】図2のスイッチの処理を説明するためのフローチャートである。

【符号の説明】

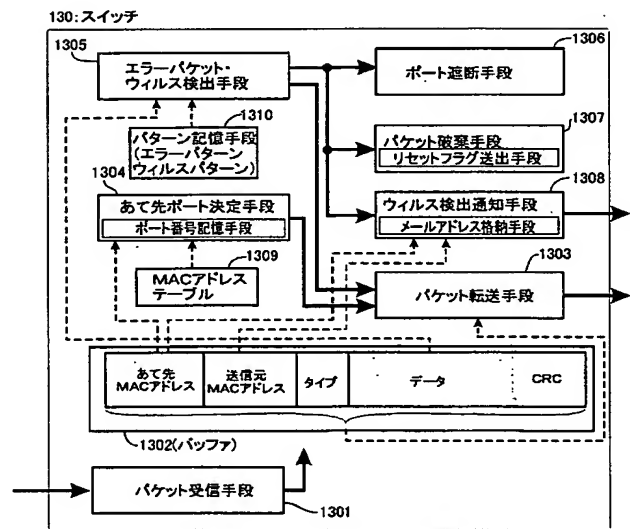
100 LAN
200 インターネット
300 ウイルスパターンデータベースサーバ
100 LAN
11 ウイルスチェックサーバ
12 コアスイッチ
151 ウイルスパターン記憶部
1413 ハブ
1412 コンピュータ
1411 コンピュータ
1423 ハブ
152 ウイルスパターン記憶部
1421 コンピュータ
1422 コンピュータ

【図1】

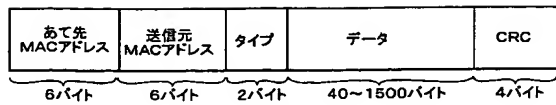


12 コアスイッチ
131, 132 (130) スイッチ
1411, 1412, 1421, 1422 端末コンピュータ
1413, 1423 ハブ
151, 152 ウイルスデータベース
1301 パケット受信手段
1302 パケットバッファ
1303 パケット転送手段
1304 あて先ポート決定手段
1305 エラーパケット・ウイルス検出手段
1306 ポート遮断手段
1307 パケット破棄手段
1308 ウイルス検出通知手段
1309 MACアドレステーブル
1310 パターン記憶手段
GW1, GW2 ゲートウェイ

【図2】



【図3】



(A)

コアシッチ12のMACアドレステーブル

ポート	MACアドレス
1	A1
2	A2
3	A3

(B)

スイッチ131のMACアドレステーブル

ポート	MACアドレス
1	B1
2	B2
3	B3

(C)

スイッチ132のMACアドレステーブル

ポート	MACアドレス
1	C1
2	C2
3	C3

(D)

【図4】

